# TOWARDS AN INFORMATION-THEORETICALLY SAFE CRYPTOGRAPHIC PROTOCOL

PEDRO FORTUNY AYUSO

Abstract. We introduce what –if some kind of group action exists– is a truly (information-theoretically) safe cryptographic communication system: a protocol which provides *zero* information to any passive adversary having full access to the channel.

## 1. The false algorithm, simple version

Assume Alice wants to share a secret $s$, which we assume for simplicity[1] is a non-zero rational number $s = p/q \in \mathbb{Q}^{\star}$. For example, $s$ could be the key of a symmetric key protocol, a password or even a complete message such as a pair of coordinates in a map or a time.

Alice picks another random rational $t$ and calls $v = (s, t)$ to the corresponding point in $\mathbb{Q}^2$.

She chooses a random transformation $A \in GL_2(\mathbb{Q})$ in the linear group of $\mathbb{Q}^2$ and computes $v_1 = v \cdot A$. Alice sends $v_1$ to Bob.

Bob picks another random transformation $B \in GL_2(\mathbb{Q})$ and computes $v_2 = v_1 \cdot B$, and sends $v_2$ back to Alice. Notice that $v_1$ gives no information to Bob or an eavesdropper (Eve) about $s$, because $t$ is random and $v_1$ can be *any* point in $\mathbb{Q}^2$, depending on $t$ and $A$, which are both unknown to both Bob and Eve. For a similar reason, the knowledge of $v_1$ and $v_2$ gives no useful information about $B$.

Alice now computes $v_3 = v_2 \cdot A^{-1}$ and sends $v_3$ back to Bob. Again, the knowledge of $v_1$, $v_2$ and $v_3$ is useless in order to retrieve the original $v$.

Finally, Bob computes $v_4 = v_3 \cdot B^{-1}$.

If only $v_4 = v$...!

## 2. The protocol “would be” safe

Let us assume the above algorithm ends up with $v_4 = v$ and let us prove its safeness under this condition.

**Theorem 1.** *The above method of communication is information-theoretically safe, assuming $v$, $A$ and $B$ (and their inverses, obviously) are kept secret. That is, the knowledge of the whole communication gives no information on the message.*

*Proof.* We only need to show that an eavesdropper which knows all the communication has no clue about what $s$ may be. In other words, it is

*Date*: March 24, 2006.

[1] This assumption might be relaxed, using an infinite set is for exposition reasons, see section 3.

enough to show that for any rational $s'$, there exist another rational number $t'$ and matrices $A'$, $B'$ such that the communication between Alice and Bob is the same (i.e. $v_1, v_2$ and $v_3$). But this is trivial. □

**Remark:** The algorithm described above obviously does not work because $GL_2(\mathbb{Q})$ is non-commutative (in general, the linear group is noncommutative for dimension greater than 1).

## 3. What is needed?

A natural question comes to mind: what are the necessary conditions for a group action on a set for the above algorithm to provide a valid system? What we used above is:

1. A set $S$ (either finite or infinite) (the rational plane in the example).
2. An action $G \times S^2 \to S^2$ of a *commutative* group $G$ on $S^2$ (the group of movements of the plane in the example, which is *not* commutative). This condition means that after the above protocol is carried out completely, one always gets the original message.
3. Conditions on the action. At least the following ones, but more might be needed:
   - Given $(s,t) \in S^2$ and $g \in G$, for any $s' \in S$ there are $t' \in S$ and $g' \in G$ such that $g \cdot (s,t) = g' \cdot (s',t')$.
   - For any $(s,t) in S^2$ and $A, B \in G$, there are $(s',t')$ and $A', B' \in G$ for which the sequences in the above algorithm are the same:
$$[(s,t)\cdot A, (s,t) \cdot A \cdot B, (s,t) \cdot A \cdot B \cdot A^{-1}] =$$
$$[(s',t') \cdot A', (s',t') \cdot A' \cdot B', (s',t') \cdot A' \cdot B' \cdot (A')^{-1}].$$

In fact, we do not need exactly an action of $G$ on $S^2$.

**Definition 1.** *Let $G$ be a (not necessarily commutative) group acting on a set $T$. We say that $t \in T$ is* comm-fixed *if $g \cdot t = t$ for any $g \in Comm(G)$ (the commutator of $G$). A subset $S \subset T$ is* comm-fixed *if any $s \in S$ is* comm-fixed.

It is clear that a subset $S \subset T$ is comm-fixed if and only if, for any $s \in S$ and any $g, h \in G$, one has $s = h^{-1}g^{-1}hg\dot{s}$. From this, it follows that we do not need exactly an action of a commutative group on $S^2$ but an action of a (not necessarily commutative) group on a set $X \supset S^2$ for which $S^2$ is comm-fixed and which satisfies, at least, condition (3) above.

We would like to prove two results; the first one seems relatively easy, while we have no clue (but are somewhat pessimistic) about the second one:

**Conjecture 1.** *With the above conditions on $X$, $S^2$ and $G$, the protocol described in section 1 is information-theoretically safe.*

**Question 1.** *Do there exist $X, S$ and a group $G$ acting on $X$ for which $S^2 \subset X$ is comm-fixed and such that the stated conditions hold?*

**Remark:** it is obvious that $S^2$ can be changed by any set of the same cardinal.

*E-mail address*: pfortuny@sdf-eu.org